UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/771,967	01/30/2001	Mehdi-Laurent Akkar	AKKAR	2638

1444 7590 03/10/2010

BROWDY AND NEIMARK, P.L.L.C.
624 NINTH STREET, NW
SUITE 300
WASHINGTON, DC 20001-5303

EXAMINER	
DAVIS, ZACHARY A	
ART UNIT	PAPER NUMBER
2437	
MAIL DATE	DELIVERY MODE
03/10/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/771,967	AKKAR ET AL.	
	Examiner	Art Unit	
	Zachary A. Davis	2437	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 December 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *15-19,22-24 and 27-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *15-19,22-24 and 27-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A response to the notice of non-compliant amendment was received on 31 December 2009. By this response, Claims 16, 19, 22, 23, 27-29, and 31-34 have been amended. No claims have been added or canceled. Claims 15-19, 22-24, and 27-34 are currently pending in the present application.

Response to Amendment

2. The declaration filed on 28 October 2009 under 37 CFR 1.131 has been considered but is ineffective to overcome the Chow reference.

The evidence submitted is insufficient to establish a reduction to practice of the invention in this country or a NAFTA or WTO member country prior to the effective date of the Chow reference. Specifically, the statement in section 8 of the declaration that the computer code of Exhibit A "implements the claimed invention" appears to be a general allegation of reduction to practice. The statement in section 8, along with the statement in section 1 that Exhibit A includes a "description of the invention", also appears to be a broad, vague, and general statement about what the exhibit describes and a general assertion that the exhibits describe a reduction to practice. However, as per MPEP § 715.07(I):

> A general allegation that the invention was completed prior to the date of the reference is not sufficient. *Ex parte Saunders*, 1883 C.D. 23, 23 O.G. 1224 (Comm'r Pat. 1883). Similarly, a declaration by the inventor to the effect that his or her invention was conceived or reduced to practice prior to the reference date,

> without a statement of facts demonstrating the correctness of this conclusion, is insufficient to satisfy 37 CFR 1.131.

The same section further states:

> The affidavit or declaration and exhibits must clearly explain which facts or data applicant is relying on to show completion of his or her invention prior to the particular date. Vague and general statements in broad terms about what the exhibits describe along with a general assertion that the exhibits describe a reduction to practice "amounts essentially to mere pleading, unsupported by proof or a showing of facts" and, thus, does not satisfy the requirements of 37 CFR 1.131(b). *In re Borkowski*, 505 F.2d 713, 184 USPQ 29 (CCPA 1974). Applicant must give a clear explanation of the exhibits pointing out exactly what facts are established and relied on by applicant. 505 F.2d at 718-19, 184 USPQ at 33. See also *In re Harry,* 333 F.2d 920, 142 USPQ 164 (CCPA 1964) (Affidavit "asserts that facts exist but does not tell what they are or when they occurred.").

Applicant's statement that the code implements the claimed invention does not, in itself, provide sufficient explanation of which parts of the code and/or summary thereof are considered to correspond to the limitations of the claimed methods. Further, the evidence presented does not clearly establish that the claimed methods (i.e. processes) were successfully performed, as required to show an actual reduction to practice (see MPEP § 2138.05(II)).

Response to Arguments

3. Applicant's arguments filed 28 October 2009 have been fully considered but they are not persuasive.

Regarding the rejection of Claims 15-19, 22-24, and 27-34 under 35 U.S.C. 103(a) as unpatentable over applicant admitted prior art in view of Chow et al, US Patent 6594761, and Kocher et al, US Patent 6278783, Applicant argues that the

declaration under 37 CFR 1.131 antedates the Chow reference (pages 8-9 of the present response). However, as detailed above, the declaration is ineffective to overcome the Chow reference.

Therefore, the Examiner maintains the rejection as set forth below.

Claim Objections

4. The objection to Claim 33 for informalities is withdrawn in light of the amendments to the claims.

Claim Rejections - 35 USC § 112

5. The rejection of Claims 15-19, 22-24, and 27-34 under 35 U.S.C. 112, second paragraph, as indefinite is NOT withdrawn. Although the amendments to the claims have corrected some of the issues of indefiniteness, the amendments have raised new issues of indefiniteness, as detailed below.

6. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

7. Claims 15-19, 22-24, and 27-34 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claim 34 recites the limitation "said second chain of operations comprising a succession of operations each corresponding to a complement of one respective operation in the first chain of operations" in lines 10-12 of the claim. It is not clear what is referred to by the phrase "one respective operation in the first chain of operations"; it is not clear if this refers to the same "one" operation for each operation in the succession of operations in the second chain or not, for example. The claim further recites "said plurality of operations comprising, for each operation of the first chain of operations, either this operation or the respective operation in the second chain of operations" in lines 21-23. The antecedent basis of the limitations "this operation" and "the respective operation" is not clear. It is not clear to which operation "this operation" is intended to refer. Similarly, it is not explicitly clear which operation in the second chain would be considered to be the "respective operation" of "this operation". This renders the claim indefinite.

Claim 19 recites that an operation in the first chain of operations includes "an operation of transfer of an intermediate result obtained from execution of an operation of said second chain of operations preceding said operation of transfer within said second chain of operations". It is not clear how an operation in the first chain would be able to operate on a result of a transfer performed in the second chain.

Claims 27 and 28 each recite "a second set of instructions for a second chain of operations". It is not clear if this is intended to refer to the same second set of instructions for the second chain of operations as recited in Claim 34. The claims also each recite "one respective operation"; it is not clear to which operation this is intended

to refer, and if this refers to the same "one" operation for each operation in the succession of operations in the first chain or not, for example.

Claim 29 recites "a second step of instructions" in line 2 and "said second step of instructions" in lines 4-5. This is generally unclear, although it appears that "step" may be intended to read "set".

Claim 31 recites "this step of determining" in lines 2-3. The reference to "this step" is somewhat uncommon, in particular with respect to the use of the pronoun "this". It is not entirely clear if "this" is being used in a manner analogous to "the" or "said" or if a different meaning is intended. The claim also recites "each selection" in line 5; it is not clear if there are plural selections referred to this claim or in Claim 34. Further, the phrase "depending of a state" in line 9 is generally unclear, although it appears that "of" may have been intended to read "on".

Claim 32 also recites "this step of determining" in lines 2-3. The reference to "this step" is somewhat uncommon, in particular with respect to the use of the pronoun "this". It is not entirely clear if "this" is being used in a manner analogous to "the" or "said" or if a different meaning is intended. The claim also recites "each selection" in line 5; it is not clear if there are plural selections referred to this claim or in Claim 34.

Claim 33 also recites "this step of determining" in lines 2-3. The reference to "this step" is somewhat uncommon, in particular with respect to the use of the pronoun "this". It is not entirely clear if "this" is being used in a manner analogous to "the" or "said" or if a different meaning is intended. The claim also recites "the selected chain of operations" in line 9; however, it appears that the selection of operations to be included

in a chain of operations would only be applicable to the third chain of operations as recited in Claim 34, which makes it unclear to which "selected chain of operations" this limitation is intended to refer.

Claims not specifically referred to above are rejected due to their dependence on a rejected base claim.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 15-19, 22-24, and 27-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over applicant admitted prior art in view of Chow et al, US Patent 6594761, and Kocher et al, US Patent 6278783.

In reference to Claim 34, Applicant admits as prior art a method including storing a first chain of operations that performs DES encryption, exchanging a message between a server entity and a microcircuit card, the server entity executing a first set of instructions applying a first chain of operations to the message to obtain a server result, the microcircuit card executing a second set of instructions applying a second chain of operations to the message to obtain a resultant message, comparing the resultant message to the server result, and the server and card mutually authenticating when the

server result and resultant message are identical (see page 2, lines 3-11, of Applicant's specification). However, Applicant's admitted prior art does not explicitly disclose determining the second chain of operations as explicitly derived from the first chain, nor that the determination is made by randomly choosing a group of operations that include some combination of operations of first and second chains of operations in either a complemented or uncomplemented state.

Chow discloses a tamper-proof encoding method that can be used with encryption protocols (see the description of application of the method to DES, starting at column 20, line 28). Chow further discloses that the encoding method includes determining whether to perform an operation or its complement (column 18, line 50-column 19, line 13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to further modify the prior art method by performing operations in either a normal or complemented state, in order to increase the tamper-resistance and obscurity of computer code (see Chow, column 4, lines 3-9). However, Chow does not explicitly disclose determining whether to perform the operation or its complement based on a random determination.

Kocher discloses a cryptographic protocol in which a chain of operations is carried out (Figures 1 and 2; column 1, line 66-column 2, line 24) and in which operations in the chain can be chosen depending on a random decision (column 9, lines 1-13). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method, described in Applicant's admitted prior art and modified by Chow, by including a random determination of whether to

perform an operation or its complement, in order to increase the security of a system (see Kocher, column 1, line 66-column 2, line 9).

In reference to Claims 15-18, Kocher further discloses that XOR operations, permutation operations, indexed access to a table, and operations that are stable with respect to XOR can be used as operations in the chain (column 2, line 44-column 3, line 9, especially column 2, lines 44-45). Chow also discloses permutations and indexed access to a table (column 18, lines 43-49; column 19, lines 52-61; column 20, lines 48-53).

In reference to Claim 19, Kocher further discloses that operations that transfer data between memory locations may be performed (column 8, lines 45-57).

In reference to Claims 22 and 31, Kocher and Chow further disclose that new operations are determined based on a random parameter (Kocher, column 9, lines 7-13, 30-48, and 62-64, where Chow discloses determining whether to perform an operation or its complement, column 18, line 50-column 19, line 13) and a counter is updated (Kocher, column 9, lines 25-27; column 10, lines 13-column 11, line 26; column 11, lines 41-45).

In reference to Claims 23 and 32, Kocher and Chow further disclose that new operations are determined based on a random parameter (Kocher, column 9, lines 7-13, 30-48, and 62-64, where Chow discloses determining whether to perform an operation or its complement, column 18, line 50-column 19, line 13) and intermediate responses are transmitted (see Kocher, column 2, lines 17-19), and Chow further discloses transmitting information with each executed operation (Chow, column 19, lines 22-34).

In reference to Claims 24 and 33, Kocher further discloses comparing a counter against a threshold value and altering operation based on the comparison (column 9, lines 25-30; see also column 7, lines 21-29).

In reference to Claim 27, Kocher further discloses performing operations byte by byte (see column 5, lines 20-27).

In reference to Claim 28, Kocher further discloses performing operations bit by bit (see column 2, line 45; also column 10, lines 51-60). Chow also discloses bit by bit operation (column 18, lines 65-66).

In reference to Claims 29 and 30, Kocher further discloses that the order of execution of operations can be permuted randomly (column 10, lines 51-55).

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of

the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Zachary A. Davis whose telephone number is (571)272-3870. The examiner can normally be reached on weekdays 9:30-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Zachary A Davis/
Primary Examiner, Art Unit 2437